Privacy Impact Assessment (PIA)

for the

Title IV Additional Servicers and Not-for-Profit Collection Agencies

September 24, 2019

For PIA Certification Updates Only: This PIA was reviewed on **September 24, 2019** by **Diana O'Hara** certifying the information contained here is valid and up to date.

Contact Point

Contact Person/Title: Greg Plenty, Supervisor, Technology Office
Contact Email: Gregory.Plenty@ed.gov

System Owner

Name/Title: Diana O'Hara
Principal Office: Federal Student Aid (FSA)

Please submit completed Privacy Impact Assessments to the Privacy Office at privacysafeguards@ed.gov

Please complete this ***Privacy Impact Assessment (PIA)*** *on how personally identifiable information (PII) is collected, stored, protected, shared, and managed electronically by your system. You may wish to consult with your ISSO in completing this document.*
If a question does not apply to your system, please answer with N/A.

1. Introduction

1.1. Describe the system including the name, acronym, and a brief description of the program or purpose for the system.

Title IV Additional Servicers (TIVAS) and Not-for-Profit Collection Agencies (NFP) are used to service Federal Student Aid (FSA) Title IV student loans. Operational capabilities of the system include borrower account management, loan conversion/de-conversion, interim/repayment servicing, payment posting, deferment and forbearance processing, letter generation, call scheduling, loan transfer/put/un-put activities, collection, skip-tracing, claims and correspondence history files. These systems communicate with the internal FSA platforms, borrowers, educational institutions, lending institutions, other loan servicers, third-party data providers, consumer reporting agencies and government agencies. Channels of communication include mail, phone calls, a secure borrower website, e-mail, and secure data transfer links.

For a complete list of the Title IV Additional Servicers and Not-for-Profit Collection Agencies (NFP) please refer to the linked attachment where you found this PIA, https://www2.ed.gov/notices/pia/index.html.

1.2. Describe the purpose for which the personally identifiable information (PII)[1] is collected, used, maintained or shared.

The PII information is used in connection with loan processing and servicing activities, such as identity verification and authentication during online account creation and telephone calls, verification between internal databases and data exchange with external trading partner databases such as:

- Consumer reporting agencies
- Lending institutions and other loan servicers
- Directory Assistance
- National Change of Address (NCOA) system
- Educational institutions

[1] The term “personally identifiable information” refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. OMB Circular A-130, page 33

1.3. Is this a new system, or one that is currently in operation?

Currently Operating System

1.4. Is this PIA new, or is it updating a previous version?

New PIA

1.5. Is the system operated by the agency or by a contractor?

Contractor

1.5.1. If the system is operated by a contractor, does the contract or other acquisition-related documents include privacy requirements?

□ N/A

Yes

2. Legal Authorities and Other Requirements

If you are unsure of your legal authority, please contact your program attorney.

2.1. What specific legal authorities and/or agreements permit and regulate the collection and use of data by the system? Please include name and citation of the authority.

The Higher Education Act of 1965 (HEA), As Amended, Section 441 and 461 Title IV, Section 401.

Executive Order 9397 (November 22, 1943), as amended by Executive Order 13478 (November 18, 2008).

SORN

2.2. Is the information in this system retrieved by an individual's name or personal identifier such as a Social Security Number or other identification?

Yes

2.2.1. If the above answer is **YES,** this system will need to be covered by Privacy Act System of Records Notice(s) (SORN(s)).[2] Please provide the SORN name, number, Federal Register citation and link, or indicate that a SORN is in progress.

□ N/A

TIVAS and NFPs are covered under the "Common Services for Borrowers" System of Records Notice (SORN), which was published as number 18-11-16 in the Federal Register on September 2, 2016 (81 FR 60683).

2.2.2. If the above answer is **NO**, explain why a SORN was not necessary. For example, the information is not retrieved by an identifier, the information is not maintained in a system of records, or the information is not maintained by the Department, etc.

☑ N/A

Click here to enter text.

Records Management
If you do not know your records schedule, please consult with your records liaison or send an email to RMHelp@ed.gov

2.3. What is the records retention schedule approved by National Archives and Records Administration (NARA) for the records contained in this system? Please provide all relevant NARA schedule numbers and disposition instructions.

TIVAS and NFPs will follow the "FSA Loan Servicing, Consolidation, and Collections Records" records schedule. DoED Record Schedule:
Schedule Locator NO: 075
Draft Date: 03/11/2009
Title: FSA Loan Servicing, Consolidation and Collections Records
Principal Office: Federal Student Aid
NARA Disposition Authority: N1-441-09-16

2.4. Is the PII contained in this system disposed of appropriately, and in accordance with the timelines in the records disposition schedule?

Yes

[2] A System of Records Notice (SORN) is a formal notice to the public that identifies the purpose for which PII is collected, from whom and what type of PII is collected, how the PII is shared externally (routine uses), and how to access and correct any PII maintained by ED. https://connected.ed.gov/om/Documents/SORN-Process.pdf

3. Characterization and Use of Information

Collection

3.1. List the specific PII elements (e.g., name, email, address, phone number, date of birth, Social Security, etc.) that the system collects, uses, disseminates, or maintains.

TIVAS and NFPs collect and maintain the employment information, educational status, family income, Social Security number (SSN), address(es), email address(es), and telephone number(s) of the individuals obligated on the debt or whose income and expenses are included in a financial statement submitted by the individual.

Records also include, but are not limited to, the application for, agreement to repay, and disbursements on the loan, and loan guaranty, if any; the repayment history, including deferments and forbearances; claims by lenders on the loan guaranty; and cancellation or discharges on grounds of qualifying service, bankruptcy discharge, disability (including medical records submitted to support application for discharge by reason of disability), death, or other statutory or regulatory grounds for relief.

Additionally, for title IV, HEA grant overpayments, the system contains records about the amount disbursed, the school that disbursed the grant, and the basis for overpayment; for all debts, the system contains demographic, employment, and other data on the individuals obligated on the debt or provided as references by the obligor, and the collection actions taken by any holder, including write-off amounts and compromise amounts.

3.2. Does the system collect only the minimum amount required to achieve the purpose stated in Question 1.2?

Yes

3.3. What are the sources of PII collected (e.g., individual, school, another agency, commercial sources, etc.)?

The information is obtained from the student/borrower, co-borrowers, co-signers, references provided by the borrower, educational institutions, financial institutions, employers, the U.S. Department of Education (DoED), the National Student Loan Data System (NSLDS), National Student Clearinghouse (NSC), and external databases (e.g., Directory Assistance, consumer reporting agencies, skip-trace vendors, U.S. Military, commercial person locator services, and U.S. Department of the Treasury).

3.4. How is the PII collected from the stated sources listed in Question 3.3 (e.g., paper form, web page, database, etc.)?

The information is collected via the following channels:

- Phone calls with customer service agents
- Entries via the Interactive Voice Response (IVR) service
- Incoming correspondence (e.g., via U.S. mail, email, etc.)
- Entry via the Borrower Portal Web site
- Bulk file transfer from third-party data providers as required, secure data transmission from DoED applications, such as: NSLDS and Debt Management Collection System (DMCS), etc.
- Secure data transmission from the U.S. Department of the Treasury.

3.5. How is the PII validated or confirmed to ensure the integrity of the information collected?[3] Is there a frequency at which there are continuous checks to ensure the PII remains valid and accurate?

The information is validated via identity verification and authentication during on-line account creation and telephone calls, verification between internal databases within systems, and data exchange with external trading partner databases such as:

- Consumer reporting agencies
- Other loan servicers
- Directory Assistance
- National Change of Address (NCOA) system

Use

3.6. Describe how the PII is used to achieve the purpose stated in Question 1.2 above.

The information is necessary to uniquely identify borrowers and to service their student loans on behalf of Federal Student Aid. The databases used by TIVAS and NFPs help track information pertinent to the borrower as well as information needed to process and service student loans throughout the loan life cycle. Collection of this information protects Federal Student Aid's fiscal interest by supporting timely and full repayment of loans and enables TIVAS and NFPs to assist borrowers with managing their loans. The information is also needed to determine borrower eligibility for entitlements such as

[3] Examples include restricted form filling, account verification, editing and validating information as it's collected, and communication with the individual whose information it is.

deferments, forbearances, discharges and to locate borrowers in cases of invalid addresses and/or telephone numbers.

3.7. Is the system using PII for testing/researching new applications or information systems prior to deployment or for training employees?

No

3.7.1. If the above answer is **YES,** what controls are in place to minimize the risk and protect the data?

☑ N/A

Click here to enter text.

Social Security Numbers

<u>It is the Department's Policy that, in order to collect Social Security Numbers, the System Owner must state the collection is: 1) authorized by law, 2) necessary for an agency purpose, and 3) there is no reasonable alternative.</u>

3.8. Does the system collect Social Security Numbers? Note that if the system maintains Social Security Numbers but does not explicitly collect them, answer 3.8.1 to address the purpose for maintaining them.

Yes

3.8.1. If the above answer is **YES**, explain the purpose for its collection, and how the SSN will be used.

□ N/A

The SSN is the unique identifier for Title IV programs and its use is required by program participants and their trading partners to satisfy borrower eligibility, loan servicing and loan status reporting requirements under law and regulations. Trading partners include the Department of Education, Internal Revenue Service (IRS), institutions of higher education, national credit bureaus, lenders and servicers.
The SSN is used for the following functions:

- To verify identity and determine eligibility to receive a benefit on a loan (such as deferment, forbearance, discharge or forgiveness)
- As a unique identifier in connection with the exchange of information between GLCS and its trading partners (e.g. educational institutions, financial institutions, loan services and consumer reporting agencies) that is performed in association with the servicing of the loans

- As a data component for submission of loan data to DoED NSLDS and Tax Form 1098-E data to the IRS
- To locate the borrower and to report and collect on the loans in case of delinquency or default.

3.8.2. Specify any alternatives considered in the collection of SNNs and why the alternatives were not selected.

□ N/A

The Social Security number is a universal way of identifying individuals and its collection and use is required for the purpose of determining an applicant's eligibility for Federal financial aid. To the extent possible, Title IV Servicers and NFPs inform the user of other unique identifiers in lieu of the SSN, such as account numbers, but the SSN is the required identifier for numerous business purposes such as those listed above.

4. Notice

4.1. How does the system provide individuals with notice about the collection of PII prior to its collection (e.g., direct notice, such as a Privacy Act Statement (if applicable) or public notice, such as a SORN, PIA,)? If notice is not provided, explain why not.

A privacy notice is presented to the borrower via the following channels:

Free Application for Federal Student Aid (FAFSA) form and on the FAFSA on line application website (https://studentaid.ed.gov/sa/privacy & https://fafsa.ed.gov/privacynotice.htm)

In order to establish an on-line account with a specific TIVAS and NFPs, the borrower must agree to the Term of Service, which incorporates the privacy policy by reference and link.

TIVAS and NFPs will send a written Privacy Notice to borrowers when they initially convert to the PCA system and annually thereafter.

4.2. Provide the text of the notice or the link to the webpage where the notice is posted if notice is provided other than by SORN or PIA.

□ N/A

To view the privacy notices for each TIVAS or NFP, please refer to the websites provided on the list of TIVAS and NFPs, found at https://www2.ed.gov/notices/pia/index.html.

4.3. What opportunities are available for individuals to consent to uses (including new uses of previously collected PII), decline to provide PII, or opt out of the project?

The borrower has the opportunity to decline to provide the information; however, providing certain information is required in order to (i) communicate with websites or customer service call centers, or (ii) receive certain benefits on a loan (such as deferment, forbearance, discharge, or forgiveness). Information is used only to process and service the borrower's DoED loans.

4.4. Is the notice referenced in Question 4.1 reviewed and revised when there are changes in the practice, policy, or activities that affect the PII and privacy to ensure that individuals are aware of and can consent to, where feasible, these changes?

Yes

5. Information Sharing and Disclosures

Internal

5.1. Will PII be shared internally with other ED principal offices? If the answer is **NO**, please skip to Question 5.4.

Yes

5.2. What PII will be shared and with whom?

□ N/A

This information is not ordinarily shared with other internal Department offices for programmatic purposes, but information collected and maintained by TIVAS and NFPs may be shared on an occasional basis within the Department when there is a legitimate business need, as determined by the System Owner.

5.3. What is the purpose for sharing the specified PII with the specified internal organizations?

□ N/A

In the event information is shared internally within the Department, it will be to ensure the Department is efficient and effective in processing loans and other servicing activities.

External

5.4. Will the PII contained in the system be shared with external entities (e.g. another agency, school district, the public, etc.)? If the answer is **NO**, please skip to Question 6.1.

Yes

5.5. What PII will be shared and with whom? List programmatic disclosures only.[4] **Note: If you are sharing Social Security Numbers externally, please specify to whom and for what purpose**.

□ N/A

TIVAS and NFPs may share information data with the following external entities:

- Guaranty Agencies
- Collection Software Systems
- Skip-Tracing Vendors (Lexis Nexus, Accurint, CBC Innovis, Trans Union LLC, Experian, Equifax)
- Educational Institutions (to coordinate the management of the loan with the educational institution's financial office)
- Direct Loan Servicers, and other servicers
- Independent Auditors
- National Consumer Reporting Agencies (to obtain updated contact information and enrollment status)
- Person locator services (to obtain updated contact information)
- Other parties as authorized by the borrower (employers, references)
- National Change of Address (to obtain updated mailing address information)
- Optional support vendors
- Contractors Fulfillment Vendors, Universal Mail Delivery Service

SSNs may be shared with these entities for the purposes stated in Question 3.9 above.

5.6. What is the purpose for sharing the PII with the specified external entities?

□ N/A

The information is shared for the following reasons: to verify the identity of an individual; to determine program eligibility and benefits; to facilitate default reduction efforts by program participants; to enforce the conditions or terms of a loan or grant; to make, service, collect, assign, adjust, transfer, refer, or discharge a loan; to counsel a debtor in repayment efforts; to investigate possible fraud or abuse; to verify compliance with program regulations; to locate a delinquent or defaulted borrower; to prepare a debt

[4] If this information is covered by Privacy Act System of Records Notice (SORN) please list only relevant programmatic disclosures listed under the Routine Uses section.

for litigation; to prepare for, conduct, or enforce a limitation, suspension, termination, or debarment action; to ensure that program requirements are met; to verify whether a debt qualifies for discharge, cancellation, or forgiveness; to conduct credit checks; to investigation complaints, update information, or correct errors contained in Department records; to refund credit balances; and to report to the Internal Revenue Service information required by U.S.C. 6050P and 6050S.

5.7. Is the sharing with the external entities authorized?

□ N/A

Yes

5.8. Is the system able to provide and retain an account of any disclosures made and make it available upon request?

□ N/A

Yes

5.9. How is the PII shared with the external entity (e.g. email, computer match, encrypted line, etc.)?

□ N/A

The information is used to process, and service the borrower's loans as permitted by the Privacy Act of 1974. The information is only shared as required to complete the Federal Student Aid business related to the student loans. Information shared outside of the Department of Education is shared through secure encrypted transmission and email.

External users (e.g., contractors, school financial aid officers) access FSA systems and data using a username and password, and/or a PIV card and PIN number. External partners use a secure data transmission of machine-to-machine transfer with external entities such as skip-tracing vendors.

5.10. Is the sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or other type of approved sharing agreement with another agency?

□ N/A

No

5.11. Does the project place limitation on re-disclosure?

□ N/A

Yes

6. **Redress**

6.1. What are the procedures that allow individuals to access their own information?

Borrowers should contact the system manager listed in the System of Records notice listed in question 2.2 and provide their name, date of birth, Social Security number and any other identifying information requested by the Department to distinguish between individuals of the same name.

In addition, borrowers may access their own information via https://studentaid.ed.gov/sa/repay-loans/default and/or https://myeddebt.ed.gov.

6.2. What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Borrowers should contact the system manager listed in the System of Records notice listed in question 2.2 and provide their name, date of birth, Social Security number and any other identifying information requested by the Department to distinguish between individuals of the same name.

In addition, borrowers may access their own information to correct any inaccurate or erroneous records via https://studentaid.ed.gov/sa/repay-loans/default and/or https://myeddebt.ed.gov.

6.3. How does the project notify individuals about the procedures for correcting their information?

The System of Records notice listed in question 2.2 explains the procedures for correcting customer information.

7. **Safeguards**

If you are unsure which safeguards will apply, please consult with your ISSO.

7.1. Does the principal office work with their CSO/ISSO to build privacy & security into the system and build privacy extensions to the extent feasible?

Yes

7.2. Is an Authority to Operate (ATO) required?

Yes

7.3. Under NIST FIPS Pub. 199, what is the security categorization of the system: **Low, Moderate, or High?**

□ N/A

Moderate

7.4. What administrative, technical, and physical safeguards are in place to protect the information?

In accordance with the Federal Information Security Management Act of 2002 (FISMA), as amended by the Federal Information Security Modernization Act of 2014, every TIVAS and NFP must implement the management, operational and technical controls necessary to protect the information. The control implementations are documented in the respective TIVAS and NFP system security plans. In addition, in accordance with FISMA, every TIVAS and NFP must receive a signed Authority To Operate (ATO) from a designated agency official. The ATO process includes a rigorous assessment of security controls, a plan of action and milestones to remediate any identified deficiencies, and a continuous monitoring program. FISMA controls comprise a combination of management, operational and technical controls, and include the following control families: access control, awareness and training, audit and accountability, security assessment and authorization, configuration management, contingency planning, identification and authentication, incident response, maintenance, media protection, physical and environment protection, planning, personnel security, privacy, risk assessment, system and services acquisition, system and communications protection, system and information integrity, and program management.

7.5. Is the information in the system appropriately secured in accordance with the IT security requirements and procedures as required by Federal law and policy?

Yes

7.6. Has a risk assessment been conducted where appropriate security controls to protect against that risk have been identified and implemented?

Yes

7.7. Please describe any monitoring, testing or evaluation conducted on a regular basis to ensure the security controls continue to work properly at safeguarding the PII.

Security and privacy controls are monitored and tested on a regular basis. Ongoing activities include, but are not limited to, the following:

- Security and privacy documentation is updated annually
- Vulnerability scanning and penetration testing are conducted on a regular basis
- Plans of actions and milestones are created for all vulnerabilities identified
- Training is conducted at least annually
- All systems must receive an Authority to Operate at a minimum of every three years (see question 7.3 for more detail on this process)
- All major system changes must go through a rigorous configuration management process that includes testing for any security and privacy impacts
- Quarterly security and privacy forums are held by Education
- Continuous monitoring through the Department's Cybersecurity Framework Risk Scorecard provides the system owner and necessary stakeholders with a detailed view of the system's implementation of the NIST Cybersecurity Framework and associated risk level of implementation level.

8. Auditing and Accountability

8.1. How does the system owner assess and ensure that the PII is used in accordance with stated practices in this PIA?

The system owner ensures the information is used in accordance with stated practices by confirming the privacy risks are properly assessed, by ensuring Privacy Act records are maintained in accordance with the provisions of the Privacy Act and the published SORN, by ensuring appropriate security and privacy controls are implemented to restrict access, and properly managing and safeguarding PII maintained within the system. The system owner participates in all major security and privacy risk briefings, meets regularly with the ISSO, and participates in FSA's Life-cycle Management Methodology, which addresses security and privacy risks throughout the system's life-cycle. Additionally, the system owner regularly reviews signed agreements that govern data use between organizations, such as System of Records notices, memoranda of understanding, etc.

8.2. Does the system owner continuously monitor and audit the privacy controls to ensure effective implementation?

Yes

8.3. What are the privacy risks associated with this system and how are those risks mitigated?

Privacy risks include unencrypted data being transmitted, lost, stolen, or compromised.

Data breaches involving PII are potentially hazardous to both individuals and organizations. Individual harm may include identity theft, embarrassment, or financial loss. Organizational harm may include a loss of public trust,
legal liability, or remediation costs.

See Section 7 Safeguards